UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,169	02/05/2004	Anat Bremler Bar	206,443	7298

7590   01/08/2007

ABELMAN, FRAYNE & SCHWAB
666 Third Ave., 10th Floor
New York, NY 10017

EXAMINER
NGUYEN, THUONG

ART UNIT	PAPER NUMBER
2155	

MAIL DATE	DELIVERY MODE
01/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Advisory Action	10/774,169	BAR ET AL.
Before the Filing of an Appeal Brief	Examiner	Art Unit	
	Thuong (Tina) T. Nguyen	2155	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED <u>07 December 2006</u> FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

    a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.

    b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

    Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

<u>NOTICE OF APPEAL</u>

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

<u>AMENDMENTS</u>

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will <u>not</u> be entered because

    (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);

    (b) ☐ They raise the issue of new matter (see NOTE below);

    (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

    (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

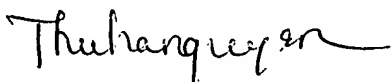   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

    The status of the claim(s) is (or will be) as follows:

    Claim(s) allowed: *None.*

    Claim(s) objected to: *None.*

    Claim(s) rejected: *1,4-26,28-35,38-60,62-69,72-94 and 96-108.*

    Claim(s) withdrawn from consideration: *None.*

<u>AFFIDAVIT OR OTHER EVIDENCE</u>

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will <u>not</u> be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will <u>not</u> be entered because the affidavit or other evidence failed to overcome <u>all</u> rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

<u>REQUEST FOR RECONSIDERATION/OTHER</u>

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.

12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____.

13. ☒ Other: <u>See Continuation Sheet.</u>

Thuhrangueyer

Primary Examiner

U.S. Patent and Trademark Office
PTOL-303 (Rev. 08-06)   Advisory Action Before the Filing of an Appeal Brief   Part of Paper No. 20070102

Continuation of 13. Other: Response to Arguments
1.   Applicant's arguments filed 12/7/06 have been fully considered, however they are not persuasive because of the following reasons:
2.   In response to applicant's argument that Lyle neither teach nor suggest monitoring the communication traffic that is directed to the addresses in the subset. In response to Applicant's argument, the Patent Office maintains the rejection because Lyle does teach monitoring the communication traffic that is directed to the addresses in the subset (figure 8 & 10; col 5, lines 12-17; Lyle discloses that the method of monitoring the network connection to send and receive information via the network and other computers). Moreover, Lyle discloses that the method of determined the baseline incident rate for affected sub-network. Therefore, Lyle already overcomes the claim limitation such as monitoring the communication traffic in the sub-network and ports.
3.   In response to applicant's argument that Lyle neither teach nor suggest identifying or choosing to monitor addresses that are expected to receive smaller amounts of communication traffic. In response to Applicant's argument, the Patent Office maintains the rejection because Lyle does teach identifying or choosing to monitor addresses that are expected to receive smaller amounts of communication traffic (figure 8; col 14, lines 56 - col 15, lines 30; Lyle discloses that the method of determined the baseline incident rate for the affected network by a prescribed amount. Lyle also discloses that the method of determined the baseline incident rate for the sub-network). Moreover, Lyle discloses the method of determine a baseline incident rate and base on the baseline rate to determined whether the number of events currently associated with the network or sub-network exceeds the baseline incident rates and determined if there is unusually or suspicious activities happened. Therefore, Lyle overcome the claim limitation such as monitoring addresses that are expected to receive smaller amounts of communication traffic.
4.   In response to applicant's argument that Lyle neither teach nor suggest applying determining that the computer has transmitted packets to a large number of different destination addresses. In response to Applicant's argument, the Patent Office maintains the rejection because Lyle does teach determining that the computer has transmitted packets to a large number of different destination addresses (col 10, lines 19-60; col 13, lines 9-21 & lines 38-55; Lyle discloses that the method of detecting the network pattern such as monitoring the rate at which the rate for that period of time exceeds by a prescribed amount the average event rate for that particular network or sub-network. Lyle also discloses that the method of detected the router ports if a particular ports is receiving an unusually high number of data packets of any type with a certain target destination or recipient address). Moreover, Lyle discloses the method of determined if the rate of certain types of messages exceeds a normal level to determined the suspicious behavior of the data packets. Therefore, Lyle already overcome the claim limitation such as determined that transmitted packets to a large number of different destination addresses.
5.   In response to applicant's argument that Lyle neither teach nor suggest filtering the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection. In response to Applicant's argument, the Patent Office maintains the rejection because Lyle does teach filtering the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection (col 14, lines 26-34; Lyle discloses that the method of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic). Moreover, Lyle discloses the method of blocking the malicious flow of network traffic. Inherently, Lyle has to filter out the malicious flow of traffic and suspicious packets.
6.   In response to applicant's argument that Lyle neither teach nor suggest detecting an increase in a rate of arrival of the packets that are indicative of the communication failure. In response to Applicant's argument, the Patent Office maintains the rejection because Lyle does teach detecting an increase in a rate of arrival of the packets that are indicative of the communication failure (col 10, lines 19 - col 11, lines 1; Lyle discloses that the method of determined if the rate of certain types of messages exceeds a normal level). Moreover, Lyle discloses the method of determined the baseline incident rate and determined if the number is increases as of determined if the packet is suspicious. Therefore, Lyle already overcome the claim limitation such as detecting an increase in a rate of arrival of the packets.
7.   In response to applicant's argument that Lyle neither teach nor suggest monitoring the communication traffic detecting ICMP unreachable. In response to Applicant's argument, the Patent Office maintains the rejection because Lyle does teach monitoring the communication traffic detecting ICMP unreachable (col 9, lines 7-37; Lyle discloses that the method of determined if the communication established or not). Therefore, Lyle already overcome the claim limitation such as determined if the ICMP unreachable.
8.   In response to applicant's argument that Lyle neither teach nor suggest detecting ill-form packets. In response to Applicant's argument, the Patent Office maintains the rejection because Lyle does teach detecting ill-form packets (col 7, lines 9-19; Lyle discloses that the method of scanning the network for the suspicious data within the tracking system). Moreover, Lyle discloses the method of detecting the suspicious attack; the suspicious attack only referred to malicious, ill-form, worm or unusually behavior packets. Inherently, Lyle includes the ill-form packets in the suspicious packets. Therefore, Lyle already overcome the claim limitation such as detecting ill-form packets.